

FILED ENTERED
LODGED RECEIVED

FEB 17 2011

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

IN THE MATTER OF THE UNITED STATES OF
AMERICA'S APPLICATION FOR A SEARCH
WARRANT TO SEIZE AND SEARCH ELECTRONIC
DEVICES FROM RESIDENCE LOCATED AT 917
212TH AVENUE NORTHEAST, SAMMAMISH,
WASHINGTON

Case No. MJ11-64
MEMORANDUM ORDER DENYING
THE GOVERNMENT'S APPLICATION
FOR A WARRANT TO SEIZE AND
SEARCH ELECTRONIC DEVICES

SEALED ORDER

I. INTRODUCTION AND SUMMARY CONCLUSION

This matter comes before the Court on the government's application for a warrant to search the residence at 917 212th Avenue Northeast, Sammamish, Washington 98074. Based on the affidavit in support of the search warrant, the home appears to be owned by Phillip and Mary Harper. Nathan Lau Affidavit, attached as Ex. 1 ("Lau Aff."), ¶¶ 27-28. However, it also appears that Joshua Cameron Smith, who is the target of the pending investigation, may live in the home with the Harpers. The nature of the relationship is unknown. *Id.*

The United States seeks authority to search the home owned by the Harpers and to seize any computers or digital devices (collectively "digital devices")¹ that may be located in the home, and to search all electronically stored information ("ESI") contained in any digital devices

¹ "Digital devices" is defined in the warrant affidavit to include any electronic device capable of processing or storing data in digital form. Lau Aff. ¶ 38 n.1.

1 seized from the home for evidence of Mr. Smith's alleged violations of 18 U.S.C. § 1030, "Fraud
2 and Related Activity in Connection with Computers." Specifically, in addition to the search of
3 the residence and the seizure of all digital devices, the application requests the authority for
4 investigative officers to: (1) search all ESI contained in the seized digital devices and related to
5 the use of the devices; (2) conduct the search without segregation by a filter team; (3) conduct
6 the search without forswearing the plain view doctrine; and (4) permit investigative agents to
7 obtain a second warrant if, during the search of the ESI, the investigating and searching agents
8 find evidence of crime outside the scope of the instant warrant. On February 7, 2011, the Court
9 advised the Assistant United States Attorney ("AUSA") that the warrant, as presented, would not
10 be granted. The United States has refused to accede to the Court's view that a filter team and
11 forswearing reliance on the plain view doctrine are appropriate, and indeed, required in this
12 specific case. Accordingly, the AUSA requested the Court to file a memorandum opinion, so
13 that the government can appeal. A copy of the requested warrant and affidavit in support is
14 attached as Exhibit 1. That request has led to this opinion.

15 Because the government, in this application, refuses to conduct its search of the digital
16 devices utilizing a filter team and forswearing reliance on the plain view doctrine, the Court
17 DENIES the application as seeking an overbroad or general warrant in violation of the Fourth
18 Amendment and the law of this Circuit.²

19
20
21
22 ² The Court is prepared to authorize the search of the residence and to seize the digital devices.
23 This opinion focuses on the search of digital devices contained in the residence. Additional changes to
the warrant regarding hash values are required, as discussed in Part II Section E of this opinion. The
Court does not understand the government to have objections to these changes, but if this is not the case,
the government should address the issue in its appeal.

1 II. DISCUSSION

2 A. *The Warrant Application to Seize and Search ESI devices*

3 The affidavit in support of the government's warrant application indicates that agents
4 received information on April 21, 2010, from Eagle View Technologies ("Eagle View") in
5 Bothell, Washington, that an intruder remotely accessed their computer server network without
6 authority on April 20, 2010, using the system logon credentials of another employee, and
7 destroyed some of the source code for a propriety software program that is the company's main
8 service product and source of revenue. In addition, the intruder may have copied some of Eagle
9 View's proprietary software or customer records, such as credit card data. Based on the Internet
10 Protocol ("IP") address of the intruder's computer from the date and time of the incident, agents
11 believe that the intruder was Joshua Cameron Smith, Eagle View's former IT systems
12 administrator who had resigned his position at Eagle View on February 26, 2010, in order to take
13 a position at another business. Lau Aff. ¶ 7.

14 Specifically, during Mr. Smith's employment for more than one year at Eagle View, Mr.
15 Smith was responsible for managing the computer equipment and software infrastructure for the
16 company, which included employee desktop computer workstations, the company network,
17 various servers and related equipment, and employee software programs. He also assigned the
18 initial passwords to all employees, and had access to their user accounts. On several occasions
19 during Mr. Smith's employment at Eagle View, he displayed a good memory and was able to
20 remember several, if not all, Eagle View employees' user names and passwords. Lau Aff. ¶ 24.
21 Although Mr. Smith's own user account had been removed from the authorized users list,
22 because Eagle View had not changed any employee or administrator passwords since Mr.
23 Smith's departure from the company, his memory of other employees' login credentials as well

1 as the administrator accounts likely enabled him to access the entire server network.

2 At 8:09 a.m. on April 20, 2010, Ms. No emailed the company's current IT Systems
3 Administrator, Jason Schrader, and IT Systems Engineer, Michael Eisenhart, asking why her
4 computer workstation had been turned off and why her user account name had been changed to
5 "admin" prior to her arrival at the office that morning. Mr. Schrader and Mr. Eisenhart
6 determined that this change indicated that a systems administrator, or at least someone with the
7 logon credentials for the "admin" user at Eagle View, had accessed Ms. No's computer after she
8 had logged off on April 19, 2010, but before she came back to the office on April 20, 2010. At
9 that time, only Mr. Smith and Mr. Eisenhart knew the local "admin" account password. Lau Aff.
10 ¶ 14.

11 Eagle View's security review revealed that an unidentified individual had used Ms. No's
12 user account to log onto Eagle View's Virtual Private Network ("VPN") at 1:50 a.m. on April
13 20, 2010, using "LogMeIn" remote access software from the IP address 173.160.192.174.
14 According to LogMeIn's records, the email address of the individual who logged into Eagle
15 View's network at that time was "raprgz@comcast.net," with a computer name of either "Josh-
16 Home" or "Josh_Home." Since that time, the email address associated with this LogMeIn
17 account was changed to "josh.smith@viridianit.com."

18 Once the intruder had successfully logged into Eagle View's network, the intruder
19 accessed various servers, including the servers that hosted Eagle View's proprietary software
20 product.³ The intruder deleted large sections of Eagle View's proprietary software product,
21

22 ³ Mr. Schrader determined that the Media Access Control ("MAC") address of the computer from
23 which the intruder accessed Eagle View's VPN was "00:1f:c6:c1:ba:0b." A MAC address is a unique
hardware identifier, similar to a serial number, associated with a particular computer. The MAC address
"00:1f:c6:c1:ba:0b" was logged by Eagle View's VPN as the computer that the intruder utilized at the
time he or she accessed Eagle View's VPN on April 20, 2010. Lau Aff. ¶ 12.

1 preventing it from functioning properly. In addition, the intruder reformatted a critical SQL
2 server hard drive, deleting approximately eighteen months worth of source code improvements,
3 historical documentation on improvements to the source code, and source code development
4 script. Eagle View President and Chief Executive Officer Chris Barrow estimated that the
5 company's damages and losses resulting from the intrusion and manipulation of their source
6 code could total from \$430,670 to \$1,670,670, depending upon the time it takes the company to
7 fully restore the software.

8 In addition to harming Eagle View's proprietary software product, the intruder accessed
9 the server which hosted Eagle View's Quickbooks application. Quickbooks contained Eagle
10 View's customer records, including credit card data. Although government agents are unable to
11 determine, based on Eagle View's server activity logs, whether the intruder copied any of Eagle
12 View's proprietary software or customer records from the Quickbooks application, they have
13 confirmed that the time and date stamps for the LogMeIn access matched the unusual VPN
14 activity, and the IP address 173.160.192.174 recorded by LogMeIn also matched the IP address
15 from the server event logs.

16 After receiving the information from Eagle View's security review discussed above,
17 government agents determined that the IP address 173.160.192.174 is owned by Comcast
18 Business Communications, Inc., and is located in the greater Seattle area. Comcast provided the
19 agents with subscriber records for that IP address, as well as the email address
20 "raprgz@comcast.net." Specifically, Comcast's records revealed that the IP address and email
21 account were both registered to "Josh Smith" at the address "917 212th Ave NE, Sammamish,
22 Washington 98074."⁴ In addition, the registrant and/or owner of the domain name
23

⁴ Government surveillance of the residence has revealed that Mr. Smith appears to reside at that

1 "viridianit.com," the email address that replaced "raprgz@comcast.net" according to LogMeIn's
2 records, was listed as "Josh Smith" at the same mailing address.

3 In addition to the computer intrusion discussed above, agents have learned someone
4 using the name "Josh Smith" from the email address "josh.smith@viridianit.com" has repeatedly
5 attempted to utilize Eagle View's Microsoft Volume Licensing account, a service through which
6 Eagle View employees can download Microsoft Corporation ("Microsoft") software titles
7 directly, in order to download Microsoft software without authority. Specifically, that individual
8 requested access to the account at 1:13 a.m. on April 20, 2010, immediately prior to the network
9 intrusion, as well as on January 13, 2011. On both dates, Eagle View received automatic email
10 messages from the Microsoft Volume Licensing Service Center notifying the company about Mr.
11 Smith's unauthorized "request for site permission."

12 Based upon this evidence, the government has applied to this Court for a warrant
13 authorizing agents to search the Harper's home and seize any evidence, fruits and
14 instrumentalities of violations of 18 U.S.C. § 1030, "Fraud and Related Activity in Connection
15 with Computers." Specifically, the government seeks authorization to search for and seize all
16 digital devices in the home to search for evidence relating to the April 20, 2010 network
17 intrusion at Eagle View, as well as search for any evidence that may be stored on the digital
18 devices. In addition, agents believe that any digital devices or storage media so seized may
19 contain source code from Eagle View's proprietary software, or Eagle View customer data, and
20 therefore request authority to search for and seize any digital devices that may contain such data.
21 Finally, the government requests authorization to search for any evidence of Microsoft software

22 _____
23 address with another couple, Phillip and Mary Harper. However, agents do not know the nature of the
Harpers' relationship with Mr. Smith, such as whether Mr. Smith is renting a portion of the home from
the Harpers. Lau Aff. ¶ 27-29.

1 that may have been downloaded and installed pursuant to Eagle View's Microsoft Volume
2 Licensing agreement after the date of Mr. Smith's February 26, 2010 resignation from the
3 company.

4 The Court finds that the warrant affidavit establishes probable cause to search the digital
5 devices located at the home for evidence of fraud and related activity committed by Mr. Smith
6 by means of the digital devices. Probable cause exists if "it would be reasonable to seek the
7 evidence in the place indicated in the affidavit." *United States v. Wong*, 334 F.3d 831, 836 (9th
8 Cir. 2003) (quoting *United States v. Peacock*, 761 F.2d 1313, 1315 (9th Cir. 1985)). Here, based
9 upon the evidence relating to Mr. Smith's employment as the IT Systems Administrator at Eagle
10 View, the evidence that the intruder's IP address was registered to Mr. Smith, as well as the fact
11 that this IP address matches the LogMeIn, VPN, and server event records for the time and date of
12 the April 20, 2010 intrusion, the Court can reasonably assume that digital devices located at Mr.
13 Smith's residence contain evidence relating to the crimes alleged.

14 However, despite the existence of probable cause to search the digital devices, the Court
15 finds the warrant requested by the government overbroad. The affidavit contains no reference to
16 use of a filter team, and no promise to forswear reliance on the plain view doctrine. With
17 respect to the procedures to be employed by law enforcement personnel to execute the search of
18 digital devices, once they have been seized, the affidavit provides:

19 In order to examine the ESI in a forensically sound manner, law
20 enforcement personnel with appropriate expertise will produce a
21 complete forensic image, if possible and appropriate, of any digital
22 device that is found to contain data or items that fall within the
23 scope of Attachment B of this Affidavit. In addition, appropriately
trained personnel may search for and attempt to recover deleted,
hidden, or encrypted data to determine whether the data fall within
the list of items to be seized pursuant to the warrant. In order to
search fully for the items identified in the warrant, law
enforcement personnel may then examine all of the data contained

1 in the forensic image/s and/or on the digital devices to view their
2 precise contents and determine whether the data falls within the list
of items to be seized pursuant to the warrant.

3 The search techniques that will be used will be only those
4 methodologies, techniques and protocols as may reasonably be
5 expected to find, identify, segregate, and/or duplicate the items
authorized to be seized pursuant to Attachment B to this affidavit.

6 If, after conducting its examination, law enforcement personnel
7 determine that any digital device is an instrumentality of the
8 criminal offense referenced above, the government may retain that
9 device during the pendency of the case as necessary to, among
10 other things, preserve the instrumentality evidence for trial, ensure
the chain of custody, and litigate the issue of forfeiture. If law
11 enforcement personnel determine that a device was not an
instrumentality of the criminal offense referenced above, it shall be
12 returned to the person/entity from whom it was seized within 90
13 days of the issuance of the warrant, unless the government seeks
and obtains authorization from the court for its retention.

14 Unless the government seeks an additional order of authorization
15 from any Magistrate Judge in the District, the government will
16 return any digital device that has been forensically copied, that is
17 not an instrumentality of the crime, and that may be lawfully
18 possessed by the person/entity from whom it was seized, to the
19 person/entity from whom it was seized within 90 days of seizure.

20 If, in the course of their efforts to search the subject digital devices,
21 law enforcement agents or analysts discover items outside of the
22 scope of the warrant that are evidence of other crimes, that
23 data/evidence will not be used in any way unless it is first
presented to a Magistrate Judge of this District and a new warrant
is obtained to seize that data, and/or to search for other evidence
related to it. In the event a new warrant is authorized, the
government may make use of the data then seized in any lawful
manner.

24 Lau Aff. ¶ 51(c)-(g).

25 As discussed below, permitting the government to conduct a search along
these lines would violate the Fourth Amendment and the law of this Circuit.

1 B. *The Fourth Amendment Prohibits General Searches*

2 The instant warrant application cannot be squared with the Fourth Amendment's
3 prohibition on general searches. The Fourth Amendment states:

4 The right of the people to be secure in their persons, houses,
5 papers, and effects, against unreasonable searches and seizures,
6 shall not be violated, and no Warrants shall issue, but upon
7 probable cause, supported by Oath or affirmation, and particularly
8 describing the place to be searched, and the persons or things to be
9 seized.

10 U.S. Const. amend. IV. The Warrant Clause of the Fourth Amendment categorically prohibits
11 the issuance of any warrant except one "particularly describing the place to be searched and the
12 persons or things to be seized." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (citing U.S.
13 Const. amend. IV). As the Supreme Court noted:

14 [t]he manifest purpose of this particularity requirement was to
15 prevent general searches. By limiting the authorization to search to
16 the specific areas and things for which there is probable cause to
17 search, the requirement ensures that the search will be carefully
18 tailored to its justifications, and will not take on the character of
19 the wide-ranging exploratory searches the Framers intended to
20 prohibit.

21 *Id.* This understanding of the Fourth Amendment's particularity requirement broke no new
22 ground. Indeed, sixty years before *Maryland v. Garrison* was decided, the Supreme Court
23 recognized general searches were long deemed to violate the Constitution. *Marron v. U.S.*, 275
U.S. 192, 196 (1927).

 The Fourth Amendment's particularity provision was enacted to respond to the evils of
general warrants and writs of assistance which English judges had employed against the
colonists. *Virginia v. Moore*, 553 U.S. 164, 169 (2008). As the Supreme Court stated:

 The practice had obtained in the colonies of issuing writs of
assistance to the revenue officers, empowering them, in their
discretion, to search suspected places for smuggled goods, which

1 James Otis pronounced “the worst instrument of arbitrary power,
2 the most destructive of English liberty and the fundamental
3 principles of law, that ever was found in an English law book;”
since they placed “the liberty of every man in the hands of every
petty officer.”

4 *Boyd v. United States*, 116 U.S. 616, 625 (1886) (internal footnotes omitted). The requirement
5 was thus designed to ensure only a specific place is searched and that probable cause to search
6 that place actually exists. *See Steele v. United States*, 267 U.S. 498, 501-02 (1925).⁵

7 Here, the government seeks permission to search every bit of data contained in each
8 digital device seized from the Harper’s home where Mr. Smith appears to reside. Contrary to the
9 Fourth Amendment’s particularity requirement limiting searches to only the specific areas and
10 things for which there is probable cause to search, the government seeks to scour everything
11 contained in the digital devices and information outside of the digital devices. This practice is
12 akin to the revenue officers in colonial days who scoured “suspected places” pursuant to a
13 general warrant.

14 The Court has considered the fact that the search warrant application seeks permission to
15 search and seize evidence of the specified crimes, and a second warrant would be needed to seize
16 evidence of other crimes for which there is no probable cause shown. However, the ability to
17 seek a second warrant after finding evidence as to which there was no probable cause to search
18 only magnifies the danger of the warrant constituting a general warrant. The requirement that a
19 second warrant be obtained provides no meaningful limitation on the scope of the search
20 conducted under the first warrant and no meaningful protection against the government obtaining
21 evidence for which it lacks probable cause. For the first warrant would be nothing more than a

22 ⁵ The Fourth Amendment’s prohibition on the issuance of general warrants goes hand in hand
23 with the requirement that each search must be carefully tailored to its justifications. Hence, even if a
warrant is not an impermissible general warrant, it still cannot be granted unless it is carefully tailored to
its justification.

1 “vehicle to gain access to data for which the government has no probable cause to collect.”

2 *Comprehensive Drug Testing v. United States*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc)

3 (“*CDT IIP*”).⁶ Indeed, the warrant the government now seeks would permit it to seize evidence

4 found outside the scope of the first warrant whether that evidence was initially in plain view, or

5 not.

6 C. *What is Involved in a Digital Search?*

7 As noted above, the search of the digital devices used by Mr. Smith would undoubtedly

8 be helpful to reveal evidence relating to the crimes alleged. Against these legitimate needs, the

9 Court weighs the vast amount and nature of data that can be stored on or accessed by personal

10 computers, an analysis which illustrates the continued importance of the Fourth Amendment’s

11 particularity requirement.

12 1. *A Digital Search Captures Vast Quantities of Data*

13 A government search of even a single, non-networked computer involves searching vast

14 quantities of ESI. As pointed out in the warrant affidavit, a single gigabyte of storage space is

15 the equivalent of 500,000 double-spaced pages of text. *Lau Aff.* ¶ 50(b). Computer hard drives

16 are now being sold for personal computers capable of storing up to two terabytes, or 2,048

17 gigabytes of data. *Id.* If a computer is networked, this exponentially increases the volume of

18 data being searched. Thus, the sheer volume of ESI involved distinguishes a digital search from

19 the search of, for example, a file cabinet.

20
21 ⁶ The Ninth Circuit’s initial panel decision is found at *Comprehensive Drug Testing v. United*
22 *States*, 473 F.3d 913 (9th Cir. 2006). This panel decision was withdrawn and superseded by
23 *Comprehensive Drug Testing v. United States*, 513 F.3d 1085 (9th Cir. 2008) (“*CDT P*”). The Ninth
Circuit then granted rehearing *en banc*, *Comprehensive Drug Testing v. United States*, 545 F.3d 1160 (9th
Cir. 2008), and issued its first *en banc* decision at *Comprehensive Drug Testing v. United States*, 579 F.3d
989 (9th Cir. 2009) (“*CDT IP*”). The initial *en banc* decision was then revised and superseded by *CDT III*,
621 F.3d 1162.

2. *A Digital Search Captures Innocent and Personal Information With No Relevance to the Asserted Crimes*

Because it is common practice for people to store innocent and deeply personal information on their personal computers, a digital search of ESI will also frequently involve searching personal information relating to the subject of the search as well as third parties. As Judge Kleinfeld noted:

The importance of this case is considerable because, for most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests - including perfect strangers - are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation.

There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality in allowing search warrants. Emails and history links may show that someone is ordering medication for a disease being kept secret even from family members. Or they may show that someone's child is being counseled by parents for a serious problem that is none of anyone else's business. Or a married mother of three may be carrying on a steamy email correspondence with an old high school boyfriend. Or an otherwise respectable, middle-aged gentleman may be looking at dirty pictures. Just as a conscientious public official may be hounded out of office because a party guest found a homosexual magazine when she went to the bathroom at his house, people's lives may be ruined because of legal but embarrassing materials found on their computers. And, in all but the largest metropolitan areas, it really does not matter whether any formal charges ensue - if the police or other visitors find the material, it will be all over town and hinted at in the newspaper within a few days.

Nor are secrets the only problem. Warrants ordinarily direct seizure, not just search, and computers are often shared by family members. Seizure of a shared family computer may, though unrelated to the law enforcement purpose, effectively confiscate a professor's book, a student's almost completed Ph.D. thesis, or a business's accounts payable and receivable.

1 *U.S. v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (Kleinfeld, J., dissenting).

2 3. *Digital Devices Function as a Portal in the Age of Cloud Computing*⁷

3 The language in the instant warrant raises another significant constitutional concern
 4 related to the interactive nature of modern digital devices. These digital devices are not just
 5 repositories of data, but access points, or portals, to other digital devices and data, typically
 6 obtained through the internet or stored on a network. All data on the internet is both separate and
 7 one. The requested warrant is, in essence, boundless. This is made evident by the fact that the
 8 government seeks authorization, among other things, to obtain “[a]ny passwords, password files,
 9 test keys, encryption codes or other information necessary to access the digital device or ESI.”
 10 *Lau Aff.* ¶ 50(n).

11 This poses a multitude of problems, and it highlights the concerns raised by Judge
 12 Kleinfeld. First, once the government has all passwords, it is able to access both the Harpers’
 13 and the target’s most sensitive information. To the extent that Mr. Smith may have medical
 14 records on-line, that information is now available to the government. If either of the apparent
 15 homeowners, Mr. and Mrs. Harper, who are not alleged to be involved in any criminal activity,
 16 or Mr. Smith are sending embarrassing, private e-mail messages, that information is now
 17 available to the government. If the government wants to see what books or movies the Mr.
 18 Smith or the Harpers are reading or watching, all of this would be fair game under the warrant
 19

20 ⁷ “The term ‘cloud computing’ is based on the industry usage of a cloud as a metaphor for the
 21 ethereal internet. A cloud platform can either be external or internal. An external cloud platform is
 22 storage or software access that is essentially rented from (or outsourced to) a remote public cloud service
 23 provider, such as Amazon or Google. This software-as-a-service allows individuals and businesses to
 collaborate on documents, spreadsheets, and more, even when the collaborators are in remote locations.
 By contrast, an internal or private cloud is a cluster of servers that is networked behind an individual or
 company’s own firewall.” David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment*
Principles to Evolving Privacy Expectations in Cloud Computing, 93 MINN. L. REV. 2205, 2216 (2009)
 (internal citations omitted).

1 presented by the government. Moreover, if Mr. Smith has been looking at legal but “dirty”
2 pictures the government will know this as well, even if the Mr. Smith had intended to “throw
3 them away.” The government candidly acknowledges that its protocols “are exacting scientific
4 procedures designed to protect the integrity of evidence and recover even hidden, erased,
5 compressed, password-protected, or encrypted files.” Lau Aff. ¶ 50(a).

6 4. *A Digital Search Captures ESI of Which the User Is Unaware*

7 In addition to granting the government access to ESI that was consciously downloaded by
8 computer users, this boundless search would reveal ESI that computer users have no way of
9 knowing is stored on their device.⁸ A search of a file cabinet, in contrast, would include only
10 items put in the file cabinet by a person. A conscious, even if unknowing, act is required. This
11 act perhaps would be analogous to intentionally downloading a file. However, in contrast to the
12 conscious act of downloading a file or storing something in a file cabinet, cache files are a set of
13 files automatically stored on a user’s hard drive by a web browser to speed up future visits to the
14 same websites, without the affirmative action of downloading. *See U.S. v. Romm*, 455 F.3d 990,
15 993 n.1 (9th Cir. 2006). *See also U.S. v. Parish*, 308 F.3d 1025, 1030-31 (9th Cir. 2002). “Most
16 web browsers keep copies of all the web pages that you view up to a certain limit, so that the
17 images can be redisplayed quickly when you go back to them.” *Romm*, 455 F.3d at 993 n.1.
18 Thus, a person’s entire online viewing history can be retrieved from the cache, without any
19 affirmative act other than visiting a web page.

20 5. *A Digital Search Captures “Destroyed” Data*

21 Unlike information in a file cabinet that can simply be taken out and destroyed, ESI is

22
23 ⁸ The Ninth Circuit has defined “downloading” as “the act of manually storing a copy of an image
on the hard drive for later retrieval.” *U.S. v. Romm*, 455 F.3d 990, 994 n.3 (9th Cir. 2006). *See also U.S.*
v. Mohrbacher, 182 F.3d 1041, 1045-46 (9th Cir. 1999) (describing downloading).

1 present after attempts to destroy it. In addition to data stored in cache files, ESI can be recovered
2 from “unallocated space” on a hard drive, which “contains deleted data, usually emptied from the
3 operating system’s trash or recycle bin folder, that cannot be seen or accessed by the user
4 without the use of forensic software.” *United States v. Flyer*, No. 08-10580, slip op. at 2429 (9th
5 Cir. Feb. 8, 2011). The government knows that once ESI is created, it is very difficult to destroy,
6 and indeed, the government highlights this function. In the affidavit, the government states

7 Once created, electronically stored information (“ESI”) can be
8 stored for years in very little space and at little or no cost. A great
9 deal of ESI is created, and stored, moreover, even without a
10 conscious act on the part of the device operator. For example, files
11 that have been viewed via the Internet are sometimes automatically
12 downloaded into a temporary Internet directory or “cache,”
13 without the knowledge of the user. The browser often maintains a
fixed amount of hard drive space devoted to these files, and files
are only overwritten as they are replaced with more recently
viewed Internet pages or if a user takes steps to delete them. . . .
Even when such action [the affirmative attempts to delete] has
been deliberately taken, ESI can often be recovered, months or
even years later, using forensic tools.

14 Lau Aff. ¶ 49(a).

15 In this case, there is good reason to authorize the search of deleted and encrypted ESI.
16 Specifically retained evidence of the alleged intrusion is unlikely to have been easily stored on
17 the digital devices at this time. Evidence may very well require the examination of “deleted”
18 files. Moreover, tracking any intrusion will undoubtedly require access to specific data stored
19 perhaps only in the portions of the hard drive that store data of where the user has been.
20 However, as discussed below, this proves too much. Although the United States has been able to
21 identify the specific computer that was involved in the intrusion of the Eagle View VPN (*see* fn.
22 3 *supra*), the government seeks authority to undertake these actions with respect to all digital
23 devices in the Harper home that agents believe were accessible to Mr. Smith. Agents do not

1 intend to seize any digital devices that were solely accessible to the Harpers. Lau Aff. ¶ 51(d)..
2 In order to effectuate this, the agents hope to interview persons present at the home during the
3 search to determine whether Mr. Smith might have used the devices. Lau Aff. ¶ 50(d).
4 Nevertheless, authority is sought to seize and search all digital devices in the home. Lau Aff. ¶
5 41. Such a request sweeps into the search of a single ESI device all sites, all data, and all
6 persons that device accessed via the internet.

7 6. *General Principles of the Fourth Amendment*

8 In opposing the requirement of a filter team and forswearing reliance on the plain view
9 doctrine, the government has taken the position that the characteristics relating to digital searches
10 set forth above do not require heightened Fourth Amendment protection, citing the U.S. Supreme
11 Court's statement in *Katz v. United States* that "the Fourth Amendment protects people, not
12 places." 389 U.S. 347, 351 (1967). It contends that a digital search is no more intrusive than a
13 properly authorized search that requires officers to sift through all of an individual's papers, and
14 every possible place where such papers might be found within the home. The government also
15 cites the Ninth Circuit's statement in *United States v. Giberson* that "[w]hile it is true that
16 computers can store a large amount of material, there is no reason why officers should be
17 permitted to search a room full of filing cabinets or even a person's library for documents listed
18 in a warrant but should not be able to search a computer." 527 F.3d 882, 888 (9th Cir. 2008).

19 Following *Giberson*, however, the Ninth Circuit began to refine its analysis. In *U.S. v.*
20 *Payton*, the court explained that "*Giberson* held that computers were not entitled to a special
21 categorical protection of the Fourth Amendment. Instead, they remained subject to the Fourth
22 Amendment's overall requirement that searches be constitutionally 'reasonable.'" 573 F.3d 859,
23 863-64 (9th Cir. 2009). Under *Giberson*, "[i]f it is reasonable to believe that a computer contains

1 items enumerated in the warrant, officers may search it.” *Id.* at 864 (citing *Giberson*, 527 F.3d at
2 888). With respect to the actual search conducted by the agents, however, the *Payton* court
3 observed that “the nature of computers makes such searches so intrusive that affidavits seeking
4 warrants for the search of computers often include a limiting search protocol, and judges issuing
5 warrants may place conditions on the manner and extent of such searches, to protect privacy and
6 other important constitutional interests . . . *We believe that it is important to preserve the option*
7 *of imposing such conditions when they are deemed warranted by judicial officers authorizing the*
8 *search of computers.” Id.* at 864 (emphasis added). The *Payton* court concluded that “the
9 special considerations of reasonableness involved in the search of computers are reflected by the
10 practice, exemplified in *Giberson*, of searching officers to stop and seek an explicit warrant when
11 they encounter a computer that they have reason to believe should be searched.” *Id.* As
12 discussed further below, this refinement continued in the *CDT* line of cases.

13 D. *Comprehensive Drug Testing Inc. v. United States*

14 The unconstitutionality of the instant warrant application, as well as the application
15 presented in *CDT III*, is revealed by tracing the odyssey of the *CDT* litigation. Here, the
16 government seeks to search all data contained in digital devices seized from the home, as well as
17 information outside the devices. The government intends to perform this search without a filter
18 team to separate from the investigative agents information that is outside the scope of the
19 warrant. Additionally, the warrant does not forswear reliance on the plain view doctrine, and
20 further seeks authorization to obtain and use information found outside the scope of the initial
21 warrant whether or not that information was found in plain view.

22 With this background, the Court turns to the Ninth Circuit opinion in *CDT III*. In that
23 case, the government obtained a warrant to search CDT’s facilities limited to the records of ten

1 baseball players for whom there was probable cause to suspect of drug use. Included in the
2 warrant was a provision to allow seizure of computer records from CDT facilities for off-site
3 examination and segregation of the evidence. To justify this provision, which the government
4 acknowledged included information beyond that relevant to the investigation, the supporting
5 affidavit contained information about the difficulty and hazards of retrieving only ESI for which
6 the government had probable cause.

7 Based on these representations, a magistrate judge granted the government permission to
8 engage in a broad seizure. However, the warrant the magistrate judge authorized also contained
9 important restrictions on the handling of seized data, including review and segregation by non-
10 investigating law enforcement personnel rather than the case agents. The purpose of the
11 segregation requirement was to prevent case agents from accessing information outside the scope
12 of the warrant.

13 Utilizing this warrant, agents found at CDT's facilities the "Tracey Directory," which
14 included, among hundreds of other documents, a spreadsheet containing the names of all the
15 major league baseball players who had tested positive for steroids.⁹ The government had
16 probable cause to search and seize records of ten baseball players. After deciding it was
17 impractical to sort through the information on-site, the agents removed the data for off-site
18 review. Although the warrant required segregation and screening, the case agent ignored this
19 requirement and took control of the data.

20 Based on its search of the Tracey Directory, the government obtained additional warrants
21 to search the facilities of CDT and Quest for information regarding more baseball players who
22 they discovered had tested positive for steroids, and issued subpoenas demanding production of

23 _____
⁹ Some of these baseball players were included in the warrant, some were not.

1 the same records it had just seized. The government claimed it was justified in obtaining this
2 additional incriminating information, based on the plain view doctrine of evidence found outside
3 the scope of the warrant. In response, CDT and the baseball players' association moved for
4 return of the seized property.

5 The litigation in *CDT III* involved multiple district courts. Two district courts ordered
6 the government to return the property.¹⁰ The judges expressed grave dissatisfaction with the
7 government's conduct; some accused the government of manipulation and misrepresentations.
8 As one district judge stated in rejecting the government's arguments, "whatever happened to the
9 Fourth Amendment? Was it . . . repealed somehow?" *CDT III*, 621 F.3d at 1177 (citing *CDT I*,
10 513 F.3d at 1117).

11 The government appealed to the Ninth Circuit. In a reissued decision, the panel reversed
12 two of the district courts' orders to return the property, and held the government was bound by
13 the third court's order containing factual determinations including the government's failure to
14 comply with the warrant and that it had displayed a callous disregard for the rights of third
15 parties. *CDT I*, 513 F.3d 1085. Despite these determinations, the Ninth Circuit initially upheld
16 the seizures. The dissent strenuously argued the decision was unfounded, ignored factual
17 findings of the lower courts, and would have dire ramifications. As Judge Thomas stated,
18 "Today's decision marks the return of the prohibited general warrant through an endorsement of
19 a disguised impermissible general search warrant—a tactic we rejected in *United States v. Rettig*,
20 589 F.2d 418 (9th Cir. 1978)." *Id.* at 1143 (Thomas, J., concurring in part, dissenting in part).

21 The case was then taken *en banc*. *CDT II*, 579 F.3d 989. The *en banc* panel reversed and
22 ordered the return of all testing results, save the ten athletes named in the first warrant. The

23 ¹⁰ One judge allowed the government to retain the materials regarding the ten players identified in
the initial warrant. The subpoenas at issue were also quashed.

majority explored the government's improper conduct and further reflected on the balance between law enforcement's perhaps legitimate need to over-seize in conducting searches of ESI devices, with the Fourth Amendment's prohibition on general or overbroad searches. To strike this balance, the court directed magistrate judges to adhere to the following five guidelines:

1. Magistrate[] [Judges] should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.

2. Segregation and redaction must be either done by specialized personnel or an independent third party. If segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.

4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1006.

On September 13, 2010, the Ninth Circuit issued a revised *en banc* opinion. *CDT III*, 621 F.3d 1162. The new opinion did not change the outcome of the first *en banc* decision, but the five guidelines that were previously part of the majority decision became part of a concurring opinion authored by Chief Judge Kozinski. In his concurrence, joined by four other judges, Chief Judge Kosinski notes the guidelines are "hardly revolutionary," are "essentially *Tamura's* solution to the problem of necessary over-seizing of evidence," and also offer "the government a safe harbor, while protecting the people's right to privacy and property in their papers and

1 effects.” *Id.* at 1178, 1180 (Kozinski, C.J., concurring).

2 In the Court’s view, the Ninth Circuit’s final *en banc* opinion does not permit the
3 issuance of the warrant the government seeks in this case for four reasons. First, although the
4 five guidelines are no longer mandatory, the majority did not hold magistrate judges are
5 prohibited from employing them or that they are improper or inappropriate. Rather the Court,
6 exercising its independent judgment, as it must, has arrived at the conclusion that some of the
7 guidelines should be applied based on the specifics of the present case.¹¹ *See id.* at 1178
8 (Kozinski, C.J., concurring). It is also important to note that the Court does not and will not
9 robotically apply the five guidelines. For example, the Court is satisfied, in this particular case,
10 that the fifth guideline’s concern is met by the government’s representations that it will return the
11 devices unless they are found to be instrumentalities of the criminal offenses named in the
12 warrant.

13 Second, the warrant application in *CDT III* was drafted in a manner designed to ensure
14 that it would be lawful and comport with the requirements of the Fourth Amendment. The
15 warrant contained a panoply of safeguards absent here. As the Ninth Circuit stated “the
16 magistrate judge . . . wisely made such broad seizure subject to certain procedural safeguards.”
17 *CDT III*, 621 F.3d at 1168. Germane to the present case, these safeguards included: (1) that

18 ¹¹ Parenthetically, the Court notes the distinction between searching a “third party” computer, as
19 was the case in *CDT III*, and searching a suspect’s computer, would be a distinction without a difference.
20 First, the Ninth Circuit stated *CDT III* was “more generally . . . about the procedures and safeguards that
21 federal courts must observe in issuing and administering search warrants and subpoenas for electronically
22 stored information,” not about searches of a third party computer. *CDT III*, 621 F.3d at 1165-66. Second,
23 in rejecting the government’s argument that it could seize items in “plain view,” the Court gave several
examples including: “Can’t find the computer? Seize the Zip disks under the bed in the room where the
computer once might have been.” *Id.* at 1171. In giving this example, the Court cited to *United States v.*
Hill, 322 F.Supp.2d 1081 (C.D. Cal 2004), a case involving the search of an individual’s computer and
residence. *Id.* And third, in *CDT III*’s “concluding thoughts” section, the Ninth Circuit stated that a
broad computer search “calls for greater vigilance on the part of judicial officers in striking the right
balance between the government’s interest in law enforcement and the *right of individuals* to be free from
unreasonable searches and seizures.” *Id.* at 1177 (emphasis added).

1 investigative agents not review and segregate the data; (2) that specialized forensic computer
2 search personnel review and segregate the data and not give it to the investigative agents; and (3)
3 seized evidence outside the scope of the warrant be returned within 60 days.

4 The *CDT III* court endorsed these safeguards noting that the government's argument that
5 the investigative agents could access all data seized is nothing but "sophistry." *Id.* at 1172. As
6 the Court stated, "it would make no sense to represent that computer personnel would be used to
7 segregate data if investigative personnel were also going to access all the data seized. What
8 would be the point?" *Id.* The court found the government's failure to follow this procedural
9 protection to reach information not covered by the warrant was a "callous disregard of the Fourth
10 Amendment," not only because of the binding findings of the district court, but also as matter of
11 "simple common sense." *Id.*

12 Hence, there is nothing in *CDT III* indicating it is unwise for a magistrate judge to require
13 the warrant application contain such safeguards where requests for broad computer searches are
14 made, that such safeguards are inappropriate, or that once such safeguards are ordered, it is
15 permissible for the government to ignore them. These safeguards are particularly appropriate in
16 this case. There is no suggestion in the government's affidavit that utilizing a filter team in this
17 investigation would compromise the government's ability to prosecute this case. There is also
18 no suggestion that requiring waiver of the plain view doctrine as a *quid pro quo* for the evident
19 over-seizing will compromise the government's ability to prosecute this case.

20 In contrast to the warrants issued in *CDT III*, the government, here, applies for the
21 broadest warrant possible - the authority to search every single thing - but minus any of the
22 procedural safeguards the Ninth Circuit in *CDT III* deemed to be wise. Perhaps the government
23 believes that its promise to use "only those methodologies, techniques and protocols as may

1 reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be
2 seized” is a sufficient safeguard. *Lau Aff.* ¶ 51(d). However, such protection is illusory and
3 does not justify the government’s request to conduct a search without a filter team and to rely on
4 the plain view doctrine. Once the Court authorizes the government to search all data, the
5 government can, and will.

6 Third, the *CDT III* opinion rejected the government’s arguments that under *United States*
7 *v. Tamura*, 694 F.2d 591 (9th Cir. 1982), it did not have to return any data it found about
8 baseball players outside the scope of the first warrant because that evidence was in “plain view”
9 when agents examined the Tracey Directory. Calling this argument “too clever by half” the
10 Ninth Circuit found the “point of the *Tamura* procedures is to maintain the privacy of materials
11 that are intermingled with seizable materials, and to avoid turning a limited search . . . into a
12 general search” *CDT III*, 621 F.3d at 1170. The government’s claim that everything is in
13 “plain view” when it is given permission to search broadly would “make a mockery of *Tamura*
14 and render the carefully crafted safeguards in the Central District warrant a nullity.” *Id.* at
15 1171.¹²

16 The instant warrant application goes a step beyond the position it took in *CDT III*. In this
17 case, not only does the government refuse to fore swear reliance on the plain view doctrine, it
18 requests that it be allowed to seek a warrant that permits it to obtain a second warrant to seize
19 additional evidence whether it was found in the initial search in plain view or not.

20 And fourth, the Ninth Circuit’s “concluding thoughts” in *CDT III* put to rest any notion

21 ¹² The Court notes a generalized seizure of ESI would be justified where there is probable cause
22 to conclude that the entirety of the contents of the ESI device is evidence of crime. *Cf. United States v.*
23 *Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (“A generalized seizure of business documents may be justified if
the government establishes probable cause to believe the entire business is merely a scheme to defraud or
that all of the business’s records are likely to evidence criminal activity.”). Here, the government has not
presented any evidence that the digital devices contain only evidence of criminal activity.

1 the warrant sought here is appropriate. Broad searches of ESI devices create “a serious risk that
2 every warrant for electronic information will become, in effect, a general warrant, rendering the
3 Fourth Amendment irrelevant.” *Id.* at 1176. The Ninth Circuit further provided:

4 Once a file is examined . . . the government may claim (as it
5 did in this case) that its contents are in plain view and, if
6 incriminating, the government can keep it. Authorization to search
7 some computer files therefore automatically becomes authorization
8 to search all files in the same sub-directory, and all files in an
9 enveloping directory, a neighboring hard drive, a nearby computer
10 or nearby storage media.

11 . . .
12 . . . It is not surprising, then, that all three of the district judges
13 below were severely troubled by the government’s conduct in this
14 case. Judge Thomas, too, in his panel dissent, expressed
15 frustration with the government’s conduct and position, calling it a
16 “breathtaking expansion of the ‘plain view’ doctrine, which clearly
17 has no application to intermingled private electronic data.

18 . . .
19 We recognize the reality that over-seizing is an inherent part of
20 the electronic search process and proceed on the assumption that,
21 when it comes to the seizure of electronic records, this will be far
22 more common than in the days of paper records. This calls for
23 greater vigilance on the part of judicial officers in striking the right
balance between the government’s interest in law enforcement and
the right of individuals to be free from unreasonable searches and
seizures. The process of segregating electronic data that is seizable
from that which is not must not become a vehicle for the
government to gain access to data which it has no probable cause
to collect.

Id. at 1176-77.

18 In this case, the Court finds that the requested warrant application impermissibly grants
19 the government a general or overbroad search warrant in violation of the Constitution and the
20 law of the Circuit. The Court also reaches this conclusion while recognizing that quite often,
21 broad searches of digital devices and “over-seizing is an inherent part of the electronic search
22
23

process.”¹³ However, a balance must be struck between the government’s investigatory interests and the right of individuals to be free from unreasonable searches and seizures. Few computers are dedicated to a single purpose; rather, computers can perform many functions, such as “postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.” *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007) (citing Orin S. Kerr, *Searches and Seizures in the Digital World*, 119 Harv. L. Rev. 531, 569 (2005)). Almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation. To maintain the balance between the government’s legitimate investigatory needs and the Fourth Amendment, the Court is ready to grant the government’s instant application on the conditions set forth in this opinion. But the government, much like it did in the *CDT* line of cases, does not seek to perform the search with constitutional safeguards, i.e., a filter team or forswearing reliance on the plain view doctrine. The government’s warrant application therefore does not pass Constitutional muster, and cannot be squared with the Ninth Circuit’s opinion in *CDT III*.

E. *The Fourth Amendment and Use of “Hash Values”*

The instant warrant search protocol also purports to authorize the government to use hash values to perform the search. The government’s proposed use of hash values does not necessarily narrow the scope of the search requested. Specifically, although “hash values” can be used to exclude files that do not interest the government such as a digital device’s operating system, they can also be used to search and find evidence outside the scope of the warrant automatically and systematically. This is because most law-enforcement forensic software can automatically search for evidence of other crimes, such as child pornography, based on known

¹³ *CDT III*, 621 F.3d at 1177.

1 hash values. *See United States v. Mann*, 592 F.3d 779, 783-84 (7th Cir. 2010) (detective ignored
2 warrant limitations and conducted general search using Forensic Tool Kit (FTK) and its
3 accompanying "KFF alert system" to locate child pornography).

4 The instant warrant application proposes to use "hash values," but contained no
5 restrictions on that use, allowing the government to search for evidence of crime for which is
6 lacks probable cause, such as child pornography. Moreover, the warrant affidavit does not
7 demonstrate "hash values" exist that can be used to ferret out the evidence for which the
8 government has probable cause in this case. The Court concludes that the following language
9 must be added to the instant warrant application in order to address the problems with using hash
10 values:

11 However, these methodologies, techniques and protocols will not
12 include the use of "hash value" libraries to search the electronically
13 stored information for items that are not set forth in the items
14 authorized to be seized in Attachment B of this warrant.

15 As this new language is necessary to address both the scope and reasonableness of the search the
16 conduct seeks to conduct, it must be included in the government's ESI application.

17 III. CONCLUSION

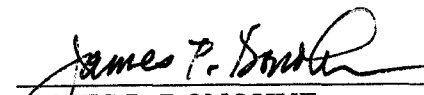
18 This Court is required under the U.S. Constitution and the law of the Circuit to deny the
19 instant warrant application. Computer fraud is a serious crime, and it appears that at least one
20 digital device was used to create substantial harm. Probable cause exists to search the digital
21 devices for evidence relating to fraud and related criminal activity. But the government asks the
22 Court to do what the law does not permit. The government would have the Court give it the
23 authority to scour all data contained in the seized digital devices, and more, without any of the
procedural protections *CDT III* deemed both wise and necessary, and the authority to obtain a
second warrant to seize any other data found outside the scope of the first warrant whether it was

1 found in plain view or not. This request is exactly what *CDT III* prohibited: "the process of
2 segregating electronic data that is seizable from that which is not must not become a vehicle for
3 the government to gain access to data which it has no probable cause to collect." *Id.* at 1177.
4 Moreover, if the Court sanctions this action, its decision effectively becomes non-reviewable.
5 *See United States v. Leon*, 468 U.S. 897 (1984).

6 *CDT III* provided strong guidance to this Court regarding ESI searches. While the
7 guidelines are not mandatory, most are appropriately required in this case. The government may
8 disagree with the decision enunciated in *CDT III*. The government's options, however, were to
9 seek review of *CDT III* with the U.S. Supreme Court or to presently comply. Neither the
10 government nor this Court has the option to pretend that *CDT III* does not exist. Because the
11 Court finds the government's warrant application, without the protections set forth in this Order,
12 fails to comply with the Fourth Amendment and the law of this Circuit, the Court DENIES the
13 government's application for a search warrant.

14 As this matter involves an on-going criminal investigation, the Clerk of Court is directed
15 to file this Order under seal. This Order will be unsealed at the earlier of when any warrant
16 relating to this matter is executed, or when a decision is made not to proceed with the
17 prosecution of the matter, or otherwise by written order. A copy of this Order shall also be
18 provided to the United States and the assigned United States District Judge.

19 DATED this 17th day of February, 2011.

20
21 
22 JAMES P. DONOHUE
23 United States Magistrate Judge